Electronic Version

Stylesheet Version v1.1.1

[Reliably Continuing a Secure Connection When The Address of a Machine at One End of the Connection Changes]

Abstract

An end machine (connected to one end of secure connection) may reliably continue to use the security association (SA) even if the self_address (usually the address of the interface) of the end machine changes. The end machine includes the new IP address in the payload of a packet (e.g., an address update message) sent to another end machine at the other end of the connection. The payload can be encrypted and authenticated to avoid third party attacks. As a result, connectivity can restored for user applications reliably and quickly without requiring substantial computations and/or data exchanges.